**Adobe AIR 3.x <= 3.2.0.2070 Múltiples Vulnerabilidades (APSB12-14)**

|  |
| --- |
| IP |
| 99.53.24.141 |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)  (CVSS2#E:F/RL:OF/RC:C) | Deacuerdo a la versión la instancia de Adobe AIR en el equipo remoto Windows es menor a la versión 3.2.0.2070 la cual se ve afectada por diversos problemas de seguridad:  - Múltiples problemas de corrupción de memoria podrían ocacionar ejecución de código arbitrario. (CVE-2012-2034,  CVE-2012-2037)  - Diversos problemas de stack overflow podrían ocacionar con ejecución de código arbitrario. (CVE-2012-2035) (CVE-2012-2036) (CVE-2012-2038) (CVE-2012-2039) |
| Solución: | | |
| Actualizar a Adobe AIR 3.3 (3.3.0.3610) o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Acceso a recursos compartidos**

|  |
| --- |
| IP |
| 99.53.24.64 |
| 99.53.24.240 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)  (CVSS2#E:F/RL:OF/RC:C) | Es posible acceder a los recursos compartidos vía SMB con las credenciales provistas. Dependiendo de los permisos, esto puede permitirá un atacante a leer/escribir información confidencial. |
| Solución: | | |
| Establecer permisos específicos de acceso, lectura y escritura para cada usuario que requiera utilizar los recursos. | | |

**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.53.24.120 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)  (CVSS2#E:F/RL:OF/RC:C) | Actualizar los controles ActiveX del host Windows remoto. Tenga en cuenta que los controles afectados son de otros fabricantes que han pedido a Microsoft a impedir que sus controles se ejecuten en Internet Explorer. |
| Solución: | | |
| Se recomienda actualizar los controles ActiveX. recordando que toda actualización puede tener impacto en los sistemas. Si la organización decide no instalar la actualización, esto debe de estar documentado.  Para más información, visite el siguiente enlace:  <http://support.microsoft.com/kb/2562937> | | |

**Adobe Acrobat Reader < 10.1.3 / 9.5.1 Múltiples Vulnerabilidades (APSB12-08)**

|  |  |
| --- | --- |
| IP | |
| 99.53.24.122 | 99.53.24.122 |
| 99.53.24.127 | 99.53.24.127 |
| 99.53.24.141 | 99.53.24.141 |
| 99.53.24.224 | 99.53.24.224 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)  (CVSS2#E:F/RL:OF/RC:C) | La versión de Adobe Reader instalada en el equipo remoto es menor a la versión 10.1.3 / 9.5.1, estas versiones se ven afectadas por múltiples vulnerabilidades:  - Un desbordamiento de enteros existe en las fuentes de letras True Type Font (TFF). (CVE-2012-0774)  - Una vulnerabilidad de corrupción de memoria existe en el manejador de JavaScript. (CVE-2012-0775)  - Un problema de seguridad existe en Adobe Reader installer el cual podría ocasionar la evasión a ciertas restricciones de seguridad.  (CVE-2012-0776) |
| Solución: | | |
| Actualizar a Adobe Reader 9.5.1 / 10.1.3 o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Adobe Flash Player <= 10.3.183.7 Múltiples Vulnerabilidades (APSB11-26)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IP** |  |  |  |  |  |
| 99.53.24.120 | 99.53.24.122 | 99.53.24.125 | 99.53.24.127 | 99.53.24.128 | 99.53.24.130 |
| 99.53.24.137 | 99.53.24.141 | 99.53.24.144 | 99.53.24.187 | 99.53.24.211 | 99.53.24.224 |
| 99.53.24.240 | 99.53.24.43 | 99.53.24.48 | 99.53.24.54 | 99.53.24.57 | 99.53.24.64 |
| 99.53.24.73 | 99.53.24.75 | 99.53.24.79 | 99.53.24.85 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de Flash Player instalada en el equipo remoto es la 10.3.183.7 o anterior. Por lo tanto ha sido reportada como vulnerable a diversas vulnerabilidades críticas:    - Ejecución de código debido a desbordamientos de memoría en la pila (StackOverflow) (CVE-2011-2426, CVE-2011-2427)    - Ejecución de código o lograr que el navegador deje de responder debido a un error de lógica. (CVE-2011-2428)    - Revelación de información al evadir un control de seguridad de Flash Player (CVE-2011-2429)    - Ejecución de código en la lógica de reproducción de multimedia (CVE-2011-2430)    - Cross Site Scripting permite a un atacante realizar acciones en nombre del usuario que sea engañado para visitar un sitio web malicioso. (CVE-2011-2444) |
| Solución: | | |
| Actualizar Adobe Flash a la versión 10.3.183.10 o posterior  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Adobe Illustrator CS5 / CS5.5 Múltiples Corrupciones de Memoria (APSB12-10)**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alto / CVSS Base Score : 7.2  (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | El equipo Windows remoto contiene una versión de Adobe Illustrator que es menor a la versión CS5 15.0.3 / CS5.5 15.1.1. Como tal, se ve afectada por diversos problemas de seguridad tales como corrupciones de memoria que podrían ocasionar la ejecución de código arbitrario en el equipo. |
| Solución: | | |
| Actualizar Adobe Illustrator CS6 (16.0) o aplicar el parche de actualización para CS5 (15.0.3) o CS5.5 (15.1.1).  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Adobe Photoshop Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alto / CVSS Base Score : 7.2  (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | La versión de Adobe Photoshop instalada en el equipo remoto es menor a la versión de CS5 12.0.5 / CS5.1 12.1.1. Dichas versiones se ven afectadas por múltiples problemas de corrupción de memoria relacionadas con el manejo de archivos .DAE y .TIF files.  Un atacante remoto podría explotar este problema al hacer que un usuario abra un archivo malicioso con extensión .DAE o .TIF, resultando en la ejecución de código arbitrario. |
| Solución: | | |
| Cualquier actualización de Adobe Photoshop CS6 (13.0) o aplicar la actualización de CS5 (12.0.5) o CS5.1 (12.1.1). | | |

**Adobe SVG posible ejecución remota de código**

|  |
| --- |
| **IP** |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alto / CVSS Base Score : 7.2  (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | La versión del visor de Adobe SVG en el equipo remoto es vulnerable a ejecución remota de código. Un atacante remoto podría explotar esta falla engañando a un usuario para que acceda a una página web especialmente diseñada. |
| Solución: | | |
| Adobe dejó de soportar el Visor SVG en enero 1, 2009. Remover el software del sistema. | | |

**Altiris AClient < 6.9.164 Múltiples Vulnerabilidades locales**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IP** |  |  |  |  |  |
| 99.53.24.122 | 99.53.24.125 | 99.53.24.127 | 99.53.24.128 | 99.53.24.130 | 99.53.24.137 |
| 99.53.24.141 | 99.53.24.144 | 99.53.24.187 | 99.53.24.211 | 99.53.24.224 | 99.53.24.240 |
| 99.53.24.43 | 99.53.24.48 | 99.53.24.54 | 99.53.24.57 | 99.53.24.64 | 99.53.24.73 |
| 99.53.24.75 | 99.53.24.79 | 99.53.24.85 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.2  (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | La versión del Agente de Altiris Client (aclient) instalado en el equipo remoto, es susceptible a un ataque que podría permitir a un usuario local elevar sus privilegios en los sistemas afectados. |
| Solución: | | |
| Actualizar Altiris Deployment Solution Agent a 6.9.164 o posterior. Se recomienda ampliamente, instalar las actualizaciones correspondientes, recordando que toda actualización puede tener impacto en los sistemas. Si la organización decide no instalar la actualización, esto debe de estar documentado.  Se recomienda visitar el siguiente enlace: http://www.symantec.com/avcenter/security/Content/2008.10.20a.html Diríjase a la sección Symantec Response.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Altiris Deployment Solution Agent < 6.9.355 elevación de privilegios localmente (SYM08-019)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP** | | | | |
| 99.53.24.122 | 99.53.24.125 | 99.53.24.127 | 99.53.24.128 | 99.53.24.130 |
| 99.53.24.137 | 99.53.24.141 | 99.53.24.144 | 99.53.24.187 | 99.53.24.211 |
| 99.53.24.224 | 99.53.24.240 | 99.53.24.48 | 99.53.24.54 | 99.53.24.57 |
| 99.53.24.64 | 99.53.24.73 | 99.53.24.75 | 99.53.24.79 | 99.53.24.85 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | La versión instalada de Altiris Deployment Solution Agent en el equipo remoto es afectada por un problema de elevación de privilegios. La explotación exitosa de este problema le puede permitir a usuarios no autorizados obtener acceso al equipo con privilegios de sistema local. |
| Solución: | | |
| Actualizar Altiris Deployment Solution 6.9 build 355 o posterior y actualizar los Agents.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Apache 2.2 < 2.2.15 Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/80** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de Apache instalada en el equipo remoto es anterior a la 2.2.15 y puede estar afectada por múltiples vulnerabilidades:  - Es posible hacer ataques de inyección de prefijos en renegociaciones TLS.  - El módulo "mod\_proxy\_ajp" regresa un código de estado equivocado.  - El módulo "mod\_isapi" intenta cargar "ISAPI.dll" cuando encuentra varios estados de error.  - Una falla en el procesamiento de código de sub-peticiones puede llevar a revelar información sensible. |
| Solución: | | |
| Actualizar a Apache versión 2.2.15 o posterior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**El agente de SNMP tiene configurada la comunidad "public"**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/161** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | Es posible obtener el nombre de la comunidad por default: "public" esta configurada en el agente del protocolo SNMP. Un atacante remoto puede utilizar esta mala configuración para obtener información sensible del sistema afectado. |
| Solución: | | |
| Cambiar el nombre de la comunidad a una personalizada por el administrador del servicio, si es posible, configurar la versión 3 de SNMP, que incluye un mecanismo de cifrado para las respuestas del servicio.  Evaluar si el servicio no es necesario y en su defecto deshabilitarlo. | | |

**Firefox < 3.5.16 Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.53.24.141 |
| 99.53.24.125 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión instalada de Firefox es anterior a la 3.15.16. Dichas versiones están afectadas por los siguientes problemas de seguridad:  - Ejecución de código debió a múltiples vulnerabilidades de corrupción de memoria.  - Un desbordamiento de memoria se dispara cuando la función "document.write()" es llamada con un string muy largo.  - Elevación de privilegios en los elementos "window.open" y "<isindex>".  - Ejecución de código arbitrario usando etiquetas HTML.  - Fuentes tipográficas descargadas podrían exponer vulnerabilidades.  - Existe una vulnerabilidad de evasión en Java cuando LiveConnect es cargado vía "data".  - Existe un error de liberación después de uso en nsDOMAttribute.  - Existe un desbordamiento de entero en NewIDArray. |
| Solución: | | |
| Actualizar a Firefox 3.5.16 o posterior. | | |

**FlexNet Connect Múltiples vulnerabilidades de ejecución de código en el servicio de actualización**

|  |
| --- |
| **IP** |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de FLEXnet Client Connect instalada en el equipo remoto incluye un control ActiveX - el "InstallShield Update Service Agent" - el cual está marcado como "seguro para scripting" y contiene varios métodos que permiten la descarga y el lanzamiento de programas arbitrarios. Si un atacante remoto logra engañar a un usuario de alguna máquina afectada para que visite una página web especialmente diseñada, podría de aprovechar este problema para ejecutar código arbitrario sujeto a los privilegios del usuario. |
| Solución: | | |
| Se recomienda ampliamente, instalar las actualizaciones correspondientes, recordando que toda actualización puede tener impacto en los sistemas. Si la organización decide no instalar la actualización, esto debe de estar documentado.  http://support.installshield.com/kb/view.asp?articleid=Q113602  http://support.installshield.com/kb/view.asp?articleid=Q113020 | | |

**Google Picasa < 3.8 Ejecución de código arbitrari en DLL**

|  |
| --- |
| **IP** |
| 99.53.24.125 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de google picasa corriendo en el equipo remoto es anterior a la 3.8. Dicha versión busca de manera insegura en su directorio de trabajo cuando resuelve dependencias de DLL.Esto puede resultar en ejecución remota de código. |
| Solución: | | |
| Actualizar la versión de Google Picasa a la 3.8 o posterior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Microsoft .NET Framework Service Pack fuera de tiempo**

|  |
| --- |
| **IP** |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | El sistema remoto tiene instalado Microsoft .NET Framework. La versión instalada no posee los service pack instalados, y si los tiene están desactualizados. |
| Solución: | | |
| Instalar la ultimo versión de service pack de Microsoft .NET Framework. | | |

**Microsoft Office Service Pack desactualizado**

|  |
| --- |
| **IP** |
| 99.53.24.43 |
| 99.53.24.127 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de Microsoft Office no tiene service pack o el que tiene ya no es soportado actualmente. |
| Solución: | | |
| Instalar la última versión de service pack | | |

**Microsoft Silverlight 4.0 < 4.0.60310 Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.53.24.122 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | El equipo remoto Microsoft Windows se encuentra ejecutando una version de Microsoft Silverligth que es afectada por múltiples vulnerabilidades:  - Una corrupción de memoria existerelacionada con un control de popup y unpropiedad llamada "DependencyProperty" (CVE-2011-1844).  - Múltiples problemas de memoria existen en la implementación del control 'DataGrid' (CVE-2011-1845). |
| Solución: | | |
| Actualizar a Silverlight 4.0.60310.0 o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Microsoft Silverlight Version NO Soportada (Windows)**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.53.24.122 | 99.53.24.125 | 99.53.24.127 | 99.53.24.128 |
| 99.53.24.130 | 99.53.24.137 | 99.53.24.141 | 99.53.24.144 |
| 99.53.24.187 | 99.53.24.211 | 99.53.24.224 | 99.53.24.240 |
| 99.53.24.43 | 99.53.24.48 | 99.53.24.54 | 99.53.24.57 |
| 99.53.24.64 | 99.53.24.73 | 99.53.24.75 | 99.53.24.79 |
| 99.53.24.85 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de Microsoft Office no tiene service pack o el que tiene ya no es soportado actualmente. |
| Solución: | | |
| Instalar la última versión de service pack | | |

**Oracle Java SE | JDK | SDK | JRE Múltiples Vulnerabilidades**

|  |  |  |
| --- | --- | --- |
| **IP** |  |  |
| 99.53.24.122 | 99.53.24.125 | 99.53.24.127 |
| 99.53.24.128 | 99.53.24.141 | 99.53.24.187 |
| 99.53.24.211 | 99.53.24.224 | 99.53.24.240 |
| 99.53.24.43 | 99.53.24.54 | 99.53.24.57 |
| 99.53.24.73 | 99.53.24.75 | 99.53.24.85 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto contiene un entorno de ejecución que se ve afectado por múltiples vulnerabilidades.  Descripción:  La versión de Oracle Java SE| JRE 6.x | JDK o Java for Business instalada en el equipo es menor a la versión 7 Update 3 / 6 Update 31 / 5.0 Update 34 / 1.4.2\_36, la cual se encuentra afectada por múltiples problemas de seguridad relacionados con los siguientes componentes:  - 2D  - AWT  - CORBA  - Concurrency  - Deployment  - I18n  - Install  - Java Runtime Environment  - Lightweight HTTP Server  - Serialization  - Sound  - Un error de stack overflow relacionado con túneles. (Bug # 6670868)  - Existe un error en relación con las excepciones de seguridad en "AnnotationInvocationHandler.getMemberMethods.  (Bug # 6761678)  - Un error en 'URI.equals "puede permitir a un valor de retorno "verdadero" cuando se manejan octetos escapado. (Bug # 7041800)  - Un error relacionado con "LiveConnect" puede causar que las cookies no sean transferidas. (Bug # 7102914)  - La conectividad SSL se rompe cuando se utiliza el sistema de codificación TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA. (Bug # 7103725) |
| Solución: | | |
| Actualizar a JDK / JRE 7 Update 3 / 6 Update 31, JDK 5.0 Update 34, SDK 1.4.2\_36 o superior y remover las versiones necesarias del equipo afectado.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

### Oracle JInitiator beans.ocx ActiveX Múltiples desbordamientos de búfer

|  |  |
| --- | --- |
| **IP** | |
| 99.53.24.85 | 99.53.24.73 |
| 99.53.24.64 | 99.53.24.43 |
| 99.53.24.240 | 99.53.24.187 |
| 99.53.24.141 | 99.53.24.128 |
| 99.53.24.122 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | El equipore remoto contiene una o mas versiones de 'beans.ocx' ActiveX control, diustribuido como parte de Oracle JInitiator.  La versión o al menos uno de los controles en el equipo se ven afectados por multiples problemas de desbordamiento de búfer, lo cual podría ocasionar en la ejecución de código arbitrario. |
| Solución: | | |
| Deshabilitar el uso de controles ActiveX hacia Internet Explorer colocando "'kill' bits". | | |

**PHP < 5.3.12 / 5.4.2 Ejecución de código**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de PHP instalado en el equipo remoto es anterior a 5.3.12 / 5.4.2, y como tal puede verse afectado por una ejecución remota de código y la vulnerabilidad de divulgación de información.  Un error en 'sapi / cgi / cgi\_main.c' el archivo puede permitir a un atacante remoto obtener el código fuente de PHP en el servidor web o ejecutar código arbitrario. En las configuraciones vulnerables, PHP trata a ciertos parámetros de cadena de consulta como argumentos de línea de comandos, incluyendo interruptores, tales como '-s', '-d', y 'C'.  Se debe tener en cuenta que esta vulnerabilidad es explotable sólo cuando PHP es utilizado en CGI. Apache con 'mod\_php' no es una configuración explotable. |
| Solución: | | |
| Actualizar PHP a la versión 5.3.12 / 5.4.2 o a la mas reciente. Tambien hay una solución disponible por el proveedor para 'mod\_rewrite'.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**RealPlayer < 15.0.2.71 Múltiples Vulnerabilidades (para Windows)**

|  |
| --- |
| **IP** |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | Deacuerdo al numero de la versión de RealPlayer, esta es menor a la versión 15.0.2.71. Dicha versión se ve afectada por múltiples vulnerabilidades:  - Existe un error relacionado con las banderas 'rvrender RMFF' , el tamaño de los arreglos en 'RV20', 'VIDOBJ\_START\_CODE', 'RV40', 'RV10', y la decodificación en 'coded\_frame\_size' 'Atrac' podrían ocasionar ejecución de código arbitrario.  (CVE-2012-0922, CVE-2012-0923, CVE-2012-0924, CVE-2012-0925, CVE-2012-0926, CVE-2012-0927, CVE-2012-0928) |
| Solución: | | |
| Actualizar a RealPlayer 15.0.2.71 o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**VLC Media Player < 2.0.2 Múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.53.24.125 |
| 99.53.24.137 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de VLC media player instalada en el equipo remoto es menor a la versión 2.0.2. Se ve afectada por diversos problemas de seguridad relacionados con problemas de heap-based buffer overflow.  Un error existe en la función 'Ogg\_DecodePacket' en el archivo 'modules/demux/ogg.c' el cual no valida de forma correcta la entrada lo cual podría ocasionar un heap-based buffer overflow, permitiendo la ejecución de código arbitrario. |
| Solución: | | |
| Actualizar a VLC Media Player 2.0.2 o superior. Alternativamente, se pueden remover los plugins que se ven afectados en el directorio de plugins de VLC's  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Winamp < 5.63 Múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.53.24.125 |
| 99.53.24.137 |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | El equipo remoto se encuentra ejecutando una versión de Winamp para Windows, esta versión se ve afectada por múltiples problemas de seguridad:  - Un problema de corrupción de memoria existe en 'in\_mod.dll' relacionado con una mala validación en el manejo de los archivos 'Impulse Tracker'.  - Diversos problemas de Heap-based buffer overflows existen en 'bmp.w5s' cuando se manejan datos de 'BI\_RGB' y 'UYVY' de archivos AVI.c  La explotación exitosa de este problema podría ocasionar la ejecución de código arbitrario en el equipo vulnerable. |
| Solución: | | |
| Actualizar a Winamp 5.63 (5.6.3.3234) o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**WinRAR < 3.71Vulnerabilidades en el Manejo de Archivos**

|  |
| --- |
| **IP** |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | La versión de WinRAR en el sistema remoto es susceptible a diversos problemas de corrupción y desbordamientos de buffer (buffer overflow). Un atacante que engañe a un usuario con un archivo malicioso podría ejecutar código con los permisos del usuario activo. |
| Solución: | | |
| Actualizar a WinRAR 3.90 o superior.  http://www.winrar.es/  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Adobe AIR < 1.5.3.9130 Múltiples Vulnerabilidades (APSB10-06)**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | La versión de Adobe AIr en el equipo remoto Windows es anterior a la 1.5.3.9130. Dichas versiones están afectadas por múltiples vulnerabilidades:  - Ataques de cross-domain requests.  - Denegación de servicio. |
| Solución: | | |
| Actualizar a Adobe AIR versión 1.5.3.9130 o posterior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Adobe Flash Player < 10.3.181.22 Múltiples vulnerabilidades**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IP** | | | | | |
| 99.53.24.120 | 99.53.24.122 | 99.53.24.125 | 99.53.24.127 | 99.53.24.128 | 99.53.24.130 |
| 99.53.24.137 | 99.53.24.141 | 99.53.24.144 | 99.53.24.187 | 99.53.24.211 | 99.53.24.224 |
| 99.53.24.240 | 99.53.24.43 | 99.53.24.48 | 99.53.24.54 | 99.53.24.57 | 99.53.24.64 |
| 99.53.24.73 | 99.53.24.75 | 99.53.24.79 | 99.53.24.85 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | Una vulnerabilidad de cross-site scripting existe en versiones de Flash Player menores a 10.3.181.22 (10.3.181.23 para ActiveX).  Un atacante podría aprovechar este problema para inyectar y ejecutar código arbitrario HTML y código script en el navegador del usuario. |
| Solución: | | |
| Actualizar a la versión más reciente de Adobe Flash 10.3.181.22 (10.3.181.23 en ActiveX) o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Apache 2.2 < 2.2.23 Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Media / CVSS Base Score : 5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N) | De acuerdo al banner la versión de Apache 2.2 es menor a la versión 2.2.23. Por lo tanto se ve afectada por múltiples problemas de seguridad:  - La utilidad 'apachectl' puede recibir un nombre de directorio LD\_LIBRARY\_PATH de longitud cero en 'envvars' mediante un archivo. Un atacante local podría explotar esta vulnerabilidad y cargar algún Dynamic Shared Object (DSO) malicioso permitiendo la ejecución remota de código. (CVE-2012-0883)  - Problemas en la validación de 'mod\_negotiation', 'Multiviews' podría permitir ataques del tipo cross-site scripting. (CVE-2012-2687) |
| Solución: | | |
| Actualizar a la versión de Apache 2.2.23 o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Certificado Digital SSL con Nombre de equipo equivocado**

|  |
| --- |
| **IP** |
| 99.53.24.171 |
| 99.53.24.169 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Media / CVSS Base Score : 5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N) | El commonNAme (CN) del certificado SSL presentadno en este puerto es diferente al del equipo. |
| Solución: | | |
| Generar un nuevo certificado digital para el servicio. | | |

**Citrix XenApp Online Plug-in / Vulnerabilidad de suplantación de identidad (MiTM) a través de certificados especialmente diseñados**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IP** | | | | | | |
| 99.53.24.85 | 99.53.24.79 | 99.53.24.75 | 99.53.24.73 | 99.53.24.64 | 99.53.24.57 | 99.53.24.54 |
| 99.53.24.48 | 99.53.24.240 | 99.53.24.224 | 99.53.24.211 | 99.53.24.187 | 99.53.24.144 | 99.53.24.141 |
| 99.53.24.137 | 99.53.24.130 | 99.53.24.128 | 99.53.24.127 | 99.53.24.125 | 99.53.24.122 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Media / CVSS Base Score : 5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N) | La versión instalada de Citrix Online Plug-in o ICA Client, en el equipo remoto cuenta con una vulnerabilidad puede ser aprovechada a través de un ataque de hombre en medio (Man in The Middle). Este problema esta reportado en el boletín MS09-056 de seguridad de Microsoft , y probablemente se deba a una falla en la detección de bytes nulos en el nombre común de un certificado. Un atacante remoto puede aprovechar esto para ejecutar un ataque "man-in-the-middle" y lograr leer o modificar el trafico de SSL/TLS al ser enviado desde el sistema. |
| Solución: | | |
| Actualizar Citrix Online Plug-in o Citrix ICA Client a la versión 11.0.150/11.2.0 o posterior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Divulgación de los archivos del respaldo de seguridad**

|  |
| --- |
| **IP** |
| 99.53.24.240 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | Un atacante puede obtener información sensible mediante los archivos de respaldo (.old, .bak, etc) que se encuentran en el servidor remoto. |
| Solución: | | |
| Asegurarse que los archivos no contengan información sensible, como credenciales de conexión a la base de datos, y borrar o proteger esos archivos que no deberían de ser accesibles. | | |

**Firefox < 4 CSS Revelación de historial de navegación**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | La instalación de Firefox 3 es potencialmente afectada por una vulnerabilidad de revelación de información.  La función JavaScript 'getComputedStyle', puede ser utilizada en un ataque cronometrado y determinar si un navegador ha visitado links de páginas. |
| Solución: | | |
| Actualizar Firefox a la versión 4.0 o posterior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Microsoft Windows Autenticación Nula en SMB**

|  |  |
| --- | --- |
| **IP** | |
| 99.53.24.171 | 99.53.24.169 |
| 99.53.24.143 | 99.53.24.135 |
| 99.53.24.134 | 99.53.24.121 |
| 99.53.24.120 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | El equipo remoto permite acceder utilizando una sesión nula de SMB. Dependiendo de la configuración un atacante podría obtener información sobre el equipo remoto. |
| Solución: | | |
| Consultar las siguientes ligas para la solución  <http://support.microsoft.com/kb/q143474/>  <http://support.microsoft.com/kb/q246261/> | | |

**PHP < 5.3.2 / 5.2.13 Múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | De acuerdo con el banner de la versión de PHP instalada en el equipo remoto es menor a 5.3.2/5.2.13. Estas versiones pueden estar afectadas por varios problemas de seguridad:  - La ruta de directorios que no terminan con '/' no pueden ser correctamente validados dentro de la función "tempnam () 'en el modo de configuración 'Safe\_mode'.  - Es posible para evitar las restricciones de seguridad de open\_basedir "/ en modo safe\_mode, 'debido a un error en la configuración sesión extendida.  - Una vulnerabilidad no especificada afecta a la entropía LCG. |
| Solución: | | |
| Actualizar a la versión más reciente provista por el fabricante.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Servidor WEB Genérico Funciones de debug habilitadas**

|  |
| --- |
| **IP** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P) | El servidor remoto tiene habilitados los métodos HTTP TRACE y/o TRACK habilitados, estos métodos son utilizados para realizar depuración de las conexión al servidor. Estos métodos pueden ser aprovechados por un atacante para realizar una ejecución cruzada de código. |
| Solución: | | |
| Consultar al fabricante y deshabilitar los métodos no requeridos en el servidor WEB. | | |

**SSL Protocolo de cifrado inseguro**

|  |
| --- |
| **IP** |
| 99.53.24.171 |
| 99.53.24.169 |
| 99.53.24.143 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El servidor remoto acepta peticiones cifradas utilizando el protocolo SSL 2.0, el cual sufre de diversas deficiencias criptográficas y se encuentra en desuso. Un atacante podría aprovechar esto para realizar un ataque de hombre en medio. |
| Solución: | | |
| Deshabilitar el soporte para SSL 2.0 y utilizar SSL3.0 o TLS 1.0 en su lugar. En el archivo de configuración httpd.conf o ssl.conf según corresponda, establecer.  SSLProtocol -ALL +SSLv3 +TLSv1  SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP | | |

**Symantec pcAnywhere vulnerabilidad en archivos CHF podría permitir una denegación de servicio**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.53.24.85 | 99.53.24.79 | 99.53.24.75 | 99.53.24.73 |
| 99.53.24.64 | 99.53.24.57 | 99.53.24.54 | 99.53.24.48 |
| 99.53.24.43 | 99.53.24.240 | 99.53.24.224 | 99.53.24.211 |
| 99.53.24.187 | 99.53.24.144 | 99.53.24.141 | 99.53.24.137 |
| 99.53.24.130 | 99.53.24.128 | 99.53.24.127 | 99.53.24.125 |
| 99.53.24.122 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P) | La versión instalada de Symantec pcAnywhere en el equipo remoto de Windows no maneja apropiadamente el formato de cadena dentro de los nombres de archivos de control remotos (.CHF) o sus rutas de archivos asociadas. Utilizando un archivo especialmente diseñado o el nombre de la ruta, un usuario local puede explotar este problema con el propósito de leer o escribir en la memoria y como mínimo lograr que la aplicación afectada deje de funcionar. |
| Solución: | | |
| Actualizar pcAnywhere a la versión 12.5.0 Build 442 (también conocido como 12.5 SP1) o posterior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Terminal Services Vulnerable a Man in The Midle (Ataque de hombre en medio)**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.53.24.83 | 99.53.24.79 | 99.53.24.77 | 99.53.24.75 |
| 99.53.24.48 | 99.53.24.43 | 99.53.24.36 | 99.53.24.227 |
| 99.53.24.226 | 99.53.24.224 | 99.53.24.187 | 99.53.24.171 |
| 99.53.24.169 | 99.53.24.141 | 99.53.24.140 | 99.53.24.137 |
| 99.53.24.130 | 99.53.24.125 | 99.53.24.120 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | El servicio Terminal Services en el host remoto es propenso a un ataque de hombre en medio y robo de sesión con lo cual un atacante podría obtener acceso al sistema con las credenciales del usuario conectado vía Terminal Service. |
| Solución: | | |
| Forzar el uso de SSL en las conexiones. Si no es posible crear un túnel de ssh para el uso del servicio. | | |

**Uso de llaves débiles para cifrado SSL**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.53.24.83 | 99.53.24.79 | 99.53.24.77 | 99.53.24.75 |
| 99.53.24.48 | 99.53.24.43 | 99.53.24.36 | 99.53.24.227 |
| 99.53.24.226 | 99.53.24.224 | 99.53.24.187 | 99.53.24.171 |
| 99.53.24.169 | 99.53.24.141 | 99.53.24.140 | 99.53.24.137 |
| 99.53.24.130 | 99.53.24.125 | 99.53.24.120 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | El sistema remoto soporta el uso de llaves SSL débiles (<=56bits) que ofrecen un cifrado débil para la comunicación de los datos. |
| Solución: | | |
| Forzar el uso de SSL en las conexiones. Si no es posible crear un túnel de ssh para el uso del servicio. | | |

**Almacenamiento de credenciales en memoria**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.53.24.85 | 99.53.24.79 | 99.53.24.75 |
| 99.53.24.73 | 99.53.24.68 | 99.53.24.64 |
| 99.53.24.57 | 99.53.24.54 | 99.53.24.48 |
| 99.53.24.43 | 99.53.24.240 | 99.53.24.224 |
| 99.53.24.211 | 99.53.24.187 | 99.53.24.144 |
| 99.53.24.141 | 99.53.24.137 | 99.53.24.130 |
| 99.53.24.128 | 99.53.24.127 | 99.53.24.125 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Baja**  Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | La llave de registro \nHKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount\nis está establecida con un valor diferente a 0, esto significa que el sistema remoto almacena locamente las contraseñas en cache para permitir el acceso automático de los usuario en caso de una falla del PDC. |
| Solución: | | |
| Establecer el valor de la llave de registro a 0 | | |

**El servicio de Terminal Services no es FIPS-140 compliant.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IP** | | | | | |
| 99.53.24.83 | 99.53.24.79 | 99.53.24.77 | 99.53.24.75 | 99.53.24.48 | 99.53.24.43 |
| 99.53.24.36 | 99.53.24.227 | 99.53.24.226 | 99.53.24.224 | 99.53.24.187 | 99.53.24.171 |
| 99.53.24.169 | 99.53.24.141 | 99.53.24.140 | 99.53.24.137 | 99.53.24.130 | 99.53.24.125 |
| 99.53.24.120 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Baja**  Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | El nivel de cifrado utilizado en el servicio de escritorio remoto no es FIPS-140 compliant. |
| Solución: | | |
| Establecer el nivel de cifrado del protocolo RDP a 4 "FIPS Compliant". | | |

**Cisco Router Vulnerabilidad en la Solicitud SNMP que permite la divulgación de información**

|  |
| --- |
| **IP** |
| 99.53.24.101 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/General** | **Baja** | Es posible determinar el modelo de equipo remoto CISCO mediante el envío de peticiones SNMP con el OID 1.3.6.1.4.1.9.1.  Un atacante puede utilizar esta información para obtener más información sobre la máquina remota. |
| Solución: | | |
| Desabilitar el servicio SNMP en el equipo remoto solo si no es utilizado o filtrar paquetes entrantes a este puerto. | | |

**El certificado digital SSL a sido firmado utilizando un algoritmo débil de hash (digestión).**

|  |
| --- |
| **IP** |
| 99.53.24.171 |
| 99.53.24.169 |
| 99.53.24.143 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Baja** | El sistema remoto utiliza un certificado digital SSL que a sido firmado utilizando una algoritmo de hash (digestión) débil como MD2, MD4, o MD5. Estos algoritmos son vulnerables a un ataque de colisión, lo que puede permitir a un atacante generar un certificado con el mismo hash (digestión) que el original y de esta manera suplantar identidades y captar trafico cifrado. |
| Solución: | | |
| Solicitar un nuevo certificado a la entidad certificadora correspondiente. | | |

**Renegociación de conexiones TLS / SSL**

|  |
| --- |
| **IP** |
| 99.53.24.171 |
| 99.53.24.169 |
| 99.53.24.143 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Baja** | La implementación de los protocolos TLS y SSL utilizados por el servidor web, falla al asociar la renegociación de handshakes de una conexión preexistente, lo que puede permitir a un atacante realizar un ataque de hombre en medio (man-in-the-middle) para insertar datos en las sesiones HTTPS y posiblemente sustraer datos transmitidos en el canal seguro, al enviar una petición no autenticada que es procesadas retroactivamente por el servidor en una post renegociación del contexto de la conexión original, generando un ataque de inyección de texto plano "plaintext injection attack", comúnmente conocido como problema del "Project Mogul". |
| Solución: | | |
| Actualizar, el servidor web y las librerías relacionadas con SSL asociadas a la ultima versión disponible.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Servicio Telnet**

|  |
| --- |
| **IP** |
| 99.53.24.101 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Baja** | El sistema remoto está ejecutando el servicio telnet. Este servicio es usado para la administración remota de equipos. La arquitectura de este servicio, lo hace inseguro ya que la comunicación en el cliente y el servidor se lleva a cabo sin ningún cifrado, esto lo hace propenso a ataques de robo de sesión, el cual permite tomar control total del sistema. |
| Solución: | | |
| Validar el uso del servicio, en caso de no ser necesario, consultar al fabricante sobre la des habilitación del servicio, si es requerido entonces establecer un filtrado para la conexión al puerto/servicio. | | |

**Soporte de envío de información en texto claro en Servicio FTP**

|  |
| --- |
| **IP** |
| 99.53.24.43 |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Baja** | El sistema remoto ejecuta el servicio de FTP, este servicio para transferencia de archivos transmite la información del usuario en texto claro, por lo que es posible interceptar las credenciales de accesos al servicio, así como los datos a través de un ataque de hombre en medio (MiTM) por medio de un sniffer en el segmento de red donde se produce la comunicación. |
| Solución: | | |
| Utilizar SFTP en lugar de este servicio o filtrar el trafico entrante al puerto o encapsular el trafico en un canal de SSL. | | |